Washington State
Military Department

Department Policy No. RSM-601-03

Subject:	Enterprise Risk Management Policy
Authorizing Source:	Chapter 4.92 RCW-Actions and Claims Against State Chapter 43.41 RCW -Risk Management Chapter 48.62 RCW - Local Government Insurance Transactions Chapter 51 RCW – Industrial Insurance State Administrative & Accounting Manual, Chapter 20 Executive Order 16-06 State Agency Enterprise Risk Management
Information Contact:	Risk Manager Building #33, Camp Murray (253) 512-7940
Effective Date:	May 15, 2011
Mandatory Review Date:	September 1, 2020
Revised:	September 1, 2016
Approved By:	Bret D. Daugherty Bret D. Daugherty, Major General The Adjutant General Washington Military Department Director

Purpose

This policy provides the risk management roles, responsibilities, and expectations for the Washington Military Department (WMD) Enterprise Risk Management (ERM) system. The ERM system includes risk assessments and mapping to analyze and determine risk priorities that assist the WMD with risk analysis and prevention efforts to minimize potential losses.

Scope

This policy applies to all WMD state employees, supervisors of state employees, volunteers and Washington National Guard while on State Active Duty status.

Definitions

Risk: Any event or outcome that has the potential to interfere with the WMD's ability to achieve its strategic and operational objectives focused on its mission.

Compliance: Risk of compliance to regulatory authority and legal actions.

Employment Practices Liability: Risks commonly associated with labor relations; recruiting; specific causes of action; workforce elements; skill-sets and capacity; and personnel actions.

Enterprise Risk Management (ERM): The management of enterprise risk through effective analysis that includes activity risk evaluation, anticipating outcomes, identifying causes, and potential mitigation strategies. ERM works to enhance WMD capability to accomplish missions and minimize potential losses.

Financial Risks: Risks associated with internal controls maintained in compliance with best business practices, externally funding requirements, major areas of financial risk, and audit findings.

Hazards: Risk of costs associated with property losses, liability, personal injury, and workers' compensation.

Loss History: WMD loss history is information received, developed, or maintained by the Office of Financial Management (OFM) Risk Management Division (RMD) and the WMD.

Risk Oversight Group (ROG): A group comprised of senior-level management staff and subject matter experts that represents each division who is responsible to review potential and actual losses, and recommend a course of action to agency executive management.

Program Liability: Risk associated with various program operations, policies and procedures, staff training, and frequency of events.

Reputational Risks: Recognized as non-physical risks and mostly associated with communications, agency image, or perceptions.

Risk Appetite: The amount of risk that an organization is prepared to accept.

Risk Assessment: The process of identifying risk, its root causes, potential outcomes and possible mitigation.

Risk Mapping: A process of listing key risks for each program, and mapping the risks by potential frequency and possible severity.

Risk Register: The list of risks that have been assessed and rated by the Loss Prevention Committee.

Self-Insurance Premium: The premium paid by WMD to the OFM RMD to fund the State of Washington Self-Insurance Liability Program. This includes general liability indemnity, auto liability indemnity, and tort defense costs. It does not include insurance to cover damage to building, equipment, on Information Technology systems damaged as a result of a natural disaster, fire, cyber event, or other unforeseen circumstances.

Threat Assessment and Response Risks: Usually related to external emergency, natural disaster, and terrorist or other violent criminal activity, as well as plans for protection of employees, property and key systems, and business continuity.

Tort Claim: A formal written filing with the DES ORM (Office of Risk Management) under RCW 4.92.100 in which the claimant alleges that certain kinds of harm or damages were caused by the State of Washington its agencies, state employees, or state volunteers.

Policy

The management of risk in protecting State assets is a shared responsibility at all levels and the purpose of the policy is to implement the ERM system in WMD for evaluating possible loss exposures, mitigating loss when possible, and managing losses once they occur.

Risk is inherent in all agency operations and some risk is unavoidable. It is important that risk management activities occur to minimize potential loss in order to protect state resources, and assist the WMD in meeting strategic and operational objectives focused on its mission.

1. Enterprise Risk Management Infrastructure:
    a. Risk management policy defines ERM as a strategic practice of the organization.
    b. WMD management identifies risk as any event that could interfere with the accomplishment of the WMD's mission and goals.
    c. ERM is integrated within all divisions of the organization to reduce losses.
    d. WMD will conduct periodic evaluations and adjust its risk management program for quality and results through a ROG.
    e. The ROG is scheduled to meet quarterly, or as needed.
    f. The ROG develops the risk register utilizing the risk assessment process.
    g. The ROG assigns ownership of the risk concerns to the appropriate area for documentation of mitigations plans and results.
    h. The ROG will use a risk assessment and mapping processes to analyze risks
    i. The ROG evaluates reported incidents, reviews potential new risks for prospective losses, and develops response briefings for the Executive Management Team (EMT) on a quarterly basis or as needed.
    j. The EMT receives a briefing of the ROG risk register recommendations, and identifies and directs risk mitigation efforts as appropriate.
    k. The EMT receives a copy of the Risk Register as submitted to OFM on an annual basis.

2. Identification of risk by all programs for potential losses will be included in risk identification, assessments and mapping processes. Potential risks could include:
    a. Employment Practices Liability
    b. Vehicle Safety
    c. Program Liability
    d. Reputational Risks
    e. Threat Assessment and Response Risks
    f. Financial Risks
    g. Hazards

Roles and Responsibilities

The following individuals will have responsibility for implementing this policy to reduce risks when possible and practical:

1. The EMT supports the processes of the ROG to reduce risk of losses to the agency by

assigning ownership to appropriate divisions which determine the risk appetite and assign loss prevention activity decisions.

2. The ROG will work to minimize risk impacts of conducting business that supports the WMD's mission. The ROG is responsible to monitor division initiated process improvements that will reduce exposures that may affect the ability to accomplish the WMD's mission.

   The Assistant to The Adjutant General (ATAG) serving in the Agency Deputy Director role will act as the Sponsor of the Enterprise Risk Management Program and Risk Oversight Group.

   a. The ROG will consist of management staff as follows:

      – Risk Manager
      – Agency Contracts and Internal Controls Officer
      – Agency Financial Manager
      – Deputy Director Information Technology
      – Chief Information System Security Officer
      – Agency Public Records Officer
      – Agency Records Retention Officer
      – Facilities and Maintenance Program Manager
      – Agency State Lean Coordinator
      – Assigned Representatives from the Emergency Management Division and Washington Youth Academy

   b. ROG Members will:

      1.) Attend meetings and participate in discussions.

      2.) Vote for a concurrence/agreement on analyses and recommendations of issues discussed.

      3.) Work to support strategic goals including:

         a) Review policies, programs and procedures to identify and evaluate ERM issues.

         b) Analyze major tort claims and incidents for mitigation strategies.

         c) Advise EMT on ways to reduce or eliminate losses.

   c. The Risk Manager will provide consultation to the committee, maintain the Risk Register for EMT, create agenda, take notes for meeting minutes, and distribute agendas and minutes.

3. The Risk Manager will direct, provide consultation and coordinate WMD risk management functions.

   a. Work with the Attorney General's Office (AAG) and Office of Financial Management (OFM) Risk Management Division (RMD) OFM to assist with responses to Tort claims.

   b. Provide directions to any person requesting to file a tort claim to refer to the OFM RMD.

c. In the event of a death or serious injury to a person, or other substantial loss the Risk Manager is responsible to notify the OFM RMD and/or Labor and Industries.

d. A detailed report will be written if an alleged or suspected loss is identified to be caused at least in part by the actions of the WMD.

4. Managers and Supervisors will work with the Risk Manager, ROG, EMT, and other staff to reduce risks using the following processes:

   a. Notify the Risk Manager of changes in facilities, programs, or situations that have the potential to create new risk for the WMD or state;

   b. Report all losses, potential claim incidents, and claims, regardless of size or nature, to the risk manager;

   c. Ensure that staff and volunteers/interns comply with policy and procedures; and

   d. Make certain that students, visitors and contractors follow appropriate rules.

5. Staff members will actively participate in the reduction of risk through their daily contribution of working efficiently, safely, and conscientiously.

   a. Retain any document related to a tort claim or event that may result in a claim in accordance with Department Policy No. DIR-007-10, Management of Document Identification, Preservation, Collection and Production for Litigation, and records retention requirements.

Procedures

1. Risk Assessment

   a. Risk assessments are conducted on an annual basis with the completion and/or modification to the WMD Risk Register.

   b. Risk Ownership, once assigned by the ROG, will be listed on the Risk Register and it will be the responsibility of the Owner to evaluate, analyze and submit mitigation strategies to the ROG.

   c. The ROG will:

      1.) Review the Risk Assessment worksheet.

      2.) Assess the content to determine what action if any the committee recommends.

      3.) Include new Risks and monitor activity of all risk items on the Risk Register for mitigation.

      4.) Utilize a mapping process to determine the likelihood and impact of each identified risk.

      5.) The Risk Register is a list maintained by ROG that identifies the WMD's assessed risks, Risk Mapping scores, and recommended response for the risk to be avoided, accepted, reduced, or transferred. The ROG will identify items from this register to present to EMT who will direct agency actions. This process does not prevent a manager from taking mitigation action in the normal course of business.

2. Loss History Reports

   a. OFM RMD provides access to loss history reports that are utilized to discuss frequency and severity of losses, and to tie the lessons learned from the analysis to future strategic plans, operational goals, performance measures, and other material aspects as appropriate. Reports may include:

      1.) Published reports that will protect private information contained within the reports.

      2.) The risk analysis report provided by the Risk Manager to the ROG.

      3.) Risk analysis will consider the loss history, established goals and measurements of outcomes related to those goals.

   b. Internal loss prevention review will occur when any other substantial loss occurs because of WMD policies, litigation, defense, or other management practices. The ROG will review the report that will include:

      1.) Incident description of events;

      2.) Risk analysis identifying root causes of the event;

      3.) Review of applicable policy and practices; and

      4.) Identify whether mitigation and control efforts are working.